National Law Enforcement Communication Center

SECTOR

Radio Network User's Guide

April, 2004

NLECC User Handbook

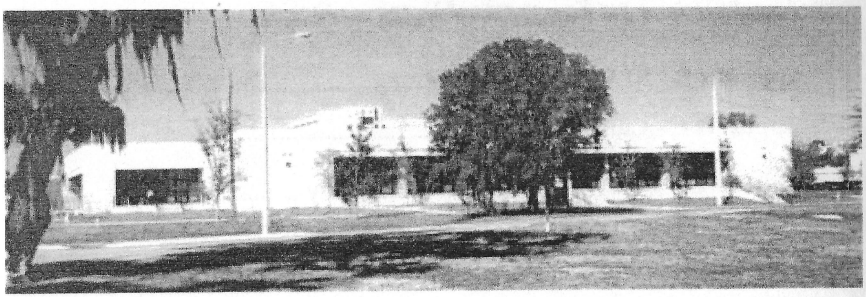
Forward

The National Law Enforcement Communications Center (NLECC) was created in 1995 at its present location in Orlando Florida. The consolidation effort was the culmination of two years of hard work, and included the relocation of a headquarters and seven field Sector organizations.

For over two decades, "Sector" and COTHEN radio communication programs have been innovative leaders in the advancement and implementation of state-of-the-art radio communications technologies. These technologies included Digital Encryption Standard (DES) voice privacy, High Frequency – Automatic Link Establishment (HF-ALE), and Over The Air Rekeying (OTAR). NLECC adds to its list of achievements as it takes its place as a technological model within the federal law enforcement community.

With the advent of new and dynamic mediums in telecommunications and land mobile radio arenas NLECC is poised on the leading edge of the law enforcement support evolution. NLECC has reaped the benefits of a cost effective consolidation process and emerged as the largest and most technologically advanced communications center in the country. By combining genuine state-of-the art equipment with many talented and knowledgeable support personnel, thousands of federal, state and local law enforcement officers are able to complete their mission in a more efficient and safe environment.

NLECC and the Sector communication program have enjoyed a long and stellar reputation, and look forward to providing the same high level of user support into the foreseeable future.



Introduction

The main objective of our nationwide VHF Radio communications network is to contribute to the success of the federal law enforcement mission by providing federal law enforcement officers, along with their state and local counterparts, a modern communications system and supporting services needed to perform their respective functions efficiently and effectively.

To meet this objective, it is necessary that our radio network meet the needs of various organizations, provide for safety of enforcement personnel where possible, and be responsive to changes in mission and objectives.

To obtain maximum value from the system, each user should have a complete and thorough understanding of the operation of the system, and of the services that are available. Because so many different agencies utilize our communications services and frequencies, it is essential that all users abide by the approved operating procedures.

The purpose of this handbook is to provide you, a subscriber of the system, with basic information on what the system is, what it can do, and how it should be utilized. This handbook is not intended as a substitute to your formal training; rather it is intended as a supplement to this training and a convenient personal source of reference. The Customs Nationwide VHF Radio Network is an important tool. When properly utilized, it can be an invaluable asset. Use it, use it often, and use it correctly – your life may depend upon it.

System Overview

The nationwide radio communications system is designed to provide radio coverage along the entire perimeter of the United States, along with any other areas where authorized users require radio coverage. The system is controlled from and by the National Law Enforcement Communications Center (NLECC) located in Orlando, Florida. It is comprised of a series of fixed radio repeaters, strategically located, that are linked directly to the NLECC (Sector) consoles. These consoles are staffed for 24-hour operation and provide a variety of essential services and emergency assistance. It is intended that the principles of radio operation, discipline, and procedures covered in this manual apply to all subscribers.

Contact Information

National Toll Free: **800-973-2867**

Direct Sector Lines:

East Team

Northeast Sector:	407-975-1740 (voice)
	407-975-2055 (fax)
Southeast Sector:	407-975-1780 (voice)
	407-975-2055 (fax)

West Team

Pacific Sector:	407-975-1800 (voice)
	407-975-1991 (fax)
Central Sector:	407-975-1760 (voice)
	407-975-1991 (fax)

SW Team

Southwest Sector (east)	407-975-1840 (voice)
	407-975-2108 (fax)
Southwest Sector (west)	407-975-1820 (voice)
	407-975-2108 (fax)

Other Numbers:

KMC hotline	877-326-5322
OTAR related matters	
Electronic Technicians	888-837-8482
User equipment and network matters	
COTHEN	800-829-6336
HF radio matters	
SIGNAL	407-975-1900
Classified message handling	
Hi-Tech Facility	407-975-1100
Annual equipment maintenance	
Training Unit	407-975-1010
Training scheduling, materials and supplies	

Sector Services

User services available from Sector are divided into primary and secondary categories. In addition to the services provided by Sector, the NLECC also provides secure High Frequency (HF) Radio support, Communications Security (COMSEC), Facsimile, and Secure Data Messaging support. Subscribers having a need for additional services should contact the NLECC to ascertain if the services can be established.

Primary Services

Emergency Assistance –
Sector will call in appropriate law enforcement officers to protect a user's personal safety or to assist with an interdiction mission. Sector will also respond when a user reports being stranded by an inoperative vehicle, vessel or aircraft.

Stop, Boarding, or Entry Support
Sector will provide status checks for all authorize users while performing suspect vehicle stops, vessel or aircraft boarding, house entry, or other potentially dangerous situation.

Query Services
Sector will provide tactical information from wide variety of law enforcement related databases in real-time. See Appendix A for a complete list of available databases and checks.

TECS Entries
While normally the responsibility of case agents, in critical, time-sensitive situations, Sector can enter information into the Treasury Enforcement Communication System

NCIC Entries
Sector will enter wanted persons, stolen articles, stolen weapons and stolen vehicles into the National Crime Information System database. Call Sector for specific data entry requirements.

Phone Service - Patches / Pages / Relays
Sector will provide phone-to-phone patches, pages and relays as necessary.

Phone Service - Other
Sector will accept collect calls, place blocked calls, place overseas phone calls and provide other miscellaneous phone services.

Portable to Portable	5 miles
Portable to Mobile	5 miles
Mobile to Mobile	30 miles
Portable to Base	15 miles
Mobile to Base	30 miles

NET Frequencies

A Repeater frequency is referred to as a NET (short for "Network) frequency, and typically named NET 1, NET 2, NET 3, etc...Typically, you would use these NET frequencies to:

- Increase your range, thus allowing you to talk to users beyond the ranges listed above
- Communicate directly with Sector, or at least have Sector monitoring your transmission
- Ensure that you can receive Sector services such as radio traffic recording and OTAR.

To utilize a NET frequency, determine which NET frequency is used in your area, and that you are in range of that repeater. On average, each repeater should cover a 30 mile radius, depending on terrain.

Once you have determined the proper channel on your radio, press the push-to-talk (PTT) button. The repeater will receive your signal and two things will happen simultaneously:

1. Your transmission will be re-transmitted (repeated) on the TAC channel that is paired to the NET channel.
2. Your transmission is sent down a phone line to Sector.

As an example, lets assume you need to talk to another user who is 30 miles away. Since this is out of the typical "TAC", range, you decide to use the local repeater, which is a NET1. You turn your radio to NET 1, then transmit. The repeater receives your signal on NET 1, converts it into TAC 1, then retransmits the signal. Simultaneously, your signal is also sent back to Sector. The user hears the transmission whether they were on NET 1 or TAC 1.

A repeater channel such as Net 1 can accommodate only one transmission at a time within the repeater's coverage area. Of course, any number can participate as long as only one transmits at any given time. Use of Net 1 can interface with a large number of TAC 1 users within the coverage area of the repeater. In fact, the repeater user may not hear some TAC 1 transmissions of other users over a

large area, and would not be aware of the resulting interference. Thus it is important that repeater (NET) channels be used only when necessary.

Radio Discipline

Discipline is the most important element in the successful operation of the Nationwide Radio Communications Network. Every individual who uses the system should be thoroughly familiar with the standards of discipline expected of all users. Users of the system should adhere to the following standards of discipline:

- All transmissions are restricted to official business
- All transmissions shall be brief. Profanities, frivolous conversations, and excessive transmission times are prohibited.
- Direct (TAC) channels will always be used instead of repeater (NET) channels in areas where direct communication is possible.
- Communications will begin with the call sign of the addressed party followed by the caller's call sign.
- Only authorized call signs are to be used.
- Only approved ten codes shall be used. (Plain language may be used)
- No classified information may be discussed over the radio system.
- The coded mode will be used for all transmissions whenever possible. Sensitive information should only be discussed in the coded mode.
- Unnecessary use of emergency procedures is prohibited.
- Radio users who have notified Sector of an emergency situation will inform Sector when the emergency has been cleared.

The enforcement of discipline on the NLECC nationwide radio communications network has been delegated to Sector. Violations of radio discipline by users will be reported to the appropriate office

or superior of the offending user for corrective action; flagrant or repetitive violations may result in disciplinary action.

Network Communication Security

All radio communications should be treated as though unauthorized persons are listening. All transmissions must be made in the coded (10-10) mode whenever possible

Other security safeguards, which should be practiced by users, are:

- No classified information will be transmitted over the system.
- Do not give our frequencies to any unauthorized individuals.
- Do not link the name of the users with the radio call sign.
- Do not pass home telephone numbers or any other personal information over unprotected frequencies.
- Do not discuss sensitive information over the radio in the clear mode.
- While in the clear mode criminal history information can only be passed over the radio in certain situations. Only criminal histories that may impact officer safety (i.e. resisting officer with violence, carrying a concealed weapon, etc.) can be passed. Other types of criminal history (i.e. forgery, DUI, etc.) cannot be passed in the clear mode.
- Whenever radios are in a public environment, caution should be taken to prevent unauthorized monitoring of traffic.

Basic Equipment Operation

There are several different types of radios that are supplied to users of our network for message transmission and reception. Basic instruction on how to operate the radio is included in the owner's manual supplied with each radio. Any additional questions concerning the operation of the equipment should be referred to your supervisor, or the local technician assigned to your area. **See Appendix B for the location and contact number for your local Radio Shop.** In addition, the NLECC Training Unit has wallet-

sized cheat sheets available for each type of radio. The Training Unit can be reached at 407-975-1010

Message Transmission Procedures

During message transmission, the following basic radio procedures shall be used. Departure from or variations in these prescribed procedures can create confusion and reduce reliability and efficiency. Where the procedure prescribed does not cover a specific operating requirement, initiative and common sense should be used.

It is fundamental that all users be familiar with radio 10-Codes and the phonetic alphabet (See page 32) and 24-hour "military" time. The phonetic alphabet is useful in interpreting the spelling of names, license plates, registration numbers, etc. The 24-hour time avoids confusion as to morning or afternoon, and the radios 10-codes are used to achieve brevity and immediate understanding.

The priority used by Sector for responding to incoming radio messages is as follows:

1. Emergency situations such as threats to life, persons in danger, and emergency medical assistance request. Typical examples include pursuits, shootings, accident scenes, etc.

2. Other urgent, and potential officer-safety situations; typically consisting of vehicle and vessel stops, boardings, residence entries, surveillances, etc.

3. Routine traffic, including pages, relays, database query request, informational calls, etc.

Important Note:
Sector supports all authorized users equally. Each operator is highly trained to receive, prioritize and handle incoming radio traffic regardless of organization, agency or position. Except in extremely rare situations, all routine radio calls are handled on a first-come, first-serve basis, and under no circumstances will take priority over an urgent call from any authorized user.

Sector asks that you please respect any requests to "stand-by". As Sector monitors the entire country, it may be possible that there is an urgent situation somewhere that is taking priority over your traffic. The Sector operator will get to your call as soon as possible.

Radio Callsigns

Radio call signs for use in the system are formatted in a standard alphanumeric sequence, which identifies the region, organization, office location, and individual user. Only authorized users of the system will be assigned call signs. The appropriate field or Headquarters organization, in accordance with the approved Standard Operating Procedure, makes call sign assignments. Sector must be notified of all call sign assignments, changes, and deletions. The NLECC (Operations Division) is responsible for radio call sign assignments to other-agency users after said users have received authorization to use the NLECC Radio Network. Generally, individual users receive their assigned call sign from their supervisor.

NOTE: Your call sign is the sole way that you will be identified on the radio network, if your call sign is incorrect, you will be denied Sector services until you can be properly identified.

Ten Codes

A standard set of 10-codes has been established for the NLECC Radio Network (See page 32). Only 10-codes on this list are authorized to be used on our network.

The purpose of these 10-codes is to allow for the efficient and effective passing of information, sometimes under radio conditions that are less than ideal.

Each user may elect to use the approved 10-codes or plain language.

Our 10-codes have been selected based on their relevance to our varied missions. Other agencies use different codes, and to prevent miscommunication, it is imperative that only our authorized 10-codes are utilized on our network.

Establishing Communications

When making a radio call, always use the other station's call sign first and your call sign last. Users will hear their own callsign and then concentrate on the call sign that follows. Using the regional prefix numbers helps to assure receipt of the alphabetical designator.

As an example, if 6A125 is calling Sector....
6A125 transmit "Sector, Six alpha one two five"
Sector response "Six alpha one two five, Sector"

In General, each user should:

- Be familiar with the call signs and locations of other users in an operation.
- Always reply to a calling station, even if only to advise it to "stand-by", unless the situation prevents it.
- Pause a second or two between transmissions so users with urgent traffic can break in.
- Always wait 1 ½ seconds after pressing the Push-to-Talk button before starting to speak.
- When transmitting, hold the microphone about six inches away and speak in a normal voice. In a noisy environment, move the microphone closer.
- Use call signs to maintain continuity as appropriate for traffic volume or as requested by Sector.
- Conduct radio checks when entering areas that may have poor reception ***before*** the start of an operation
- Acknowledge each received call, either by advising "10-4", or using some other appropriate terminology. If your transmission is unacknowledged, you must assume that the message is undelivered.

Emergency Communication Procedures

A user, who requires use of the channel on an emergency basis, while it is in use by others, should break-in during a pause between transmissions.

In an emergency, users should break-in with the word "Emergency".

All stations hearing the word "emergency" shall stop transmitting, listen carefully, and prepare to receive a message and take action. The user will then transmit the emergency message.

If there is no time to verify that the channel is clear, or to wait for a pause between transmissions, or if no response is made, it may be necessary to transmit the user's call sign, situation, location and requirements, and hope that Sector or another user has received the message. In this situation, repeating the message whenever possible will increase the probability that it will be received.

Suspicious Boarding Communication Procedures

Two-way communication is essential in suspect vehicle stops, vessel or aircraft boardings, house entries and other potentially dangerous situations. In each of these activities, users will:

- Notify Sector that the enforcement contact *will* take place and provide appropriate information. Appropriate information is information you would like Sector to have if a serious situation develops. For example, prior to a vehicle stop, specify the location, license number, description and number of occupants.
- Wait for Sector's acknowledgement.
- Within 10 minutes, or other locally accepted time interval after the enforcement contact report has been made, notify Sector of "situation clear" or other contemplated action. If the enforcement action takes longer than anticipated, advise Sector; this restarts the timing cycle.
- Sector will acknowledge and make all appropriate record system checks. In stop, boarding, entry and similar potentially dangerous situations, Sector will generally wait until the user reports he is ready before transmitting results of the record system checks. However, if an "Armed and Dangerous" notation is included in the response, Sector will attempt to call the user; in this situation the user should be especially sure the suspect cannot hear the radio before responding to Sector.
- If no "Clear" report is received after the standard or accepted time interval, Sector will call the user to verify officer status. If contact is not made after three calls, Sector will immediately arrange to speed assistance to the last reported location of the unit.
- Notify sector of 10-8 status when you clear the scene.

Over-The-Air Rekey Program

Background

The Federal Government, in collaboration with the Motorola Corporation developed Over-The-Air-Rekeying (OTAR) in the early 1990s as a means of enhancing communications security and officer safety. The early use of voice privacy on the NLECC Radio Network required encryption keys (codes) be manually loaded into each individuals radio by means of a Key Variable Loader (KVL). This was extremely labor intensive and not very practical in an operational environment.

With the advent of the OTAR system, it is now possible to use the existing radio network to perform the work of the KVL. The OTAR system uses a central computer called the Key Management Controller (KMC) and the NLECC Radio Network to transfer, load and replace voice privacy keys in large groups of radios simultaneously, and normally without any intervention on the part of the radio user.

The KMC, located at the National Law Enforcement Communications Center (NLECC) in Orlando, Florida is the computer that manages the delivery, maintenance, and placement of voice privacy keys in the vast majority of mobile, portable, and consulate radios currently in use in the field. Most key management and OTAR functions are automated and transparent to the radio user.

Clear versus Coded Transmissions

Regardless of the type of radio employed, all transmissions made in the clear or unprotected mode are capable of being intercepted by unauthorized personnel using an inexpensive scanner. NLECC Radio Network frequencies, along with those of most other law enforcement agencies, have been published in numerous publications and have been posted on the Internet. Using the direct or car-to-car mode of operation in the clear mode does not provide protection from unauthorized interception. The only means currently available to protect sensitive law enforcement communications is through the employment of voice privacy encryption, as is available on the NLECC Radio Network.

Monthly Key Changes.

Key changes occur on a monthly basis, usually the first working Monday of the month. Radios that are frequently used on direct frequencies (car-to-car) must change to a Net (Repeater) channel to

receive the new keys. If the radio is functioning on a Net channel on the day encryption keys are changed, the radio will automatically receive the updated keys.

National Key Standards – DHS Users

DHS Users on the NLECC network will utilize a standard series of voice privacy keys. This means that the exact same key is used in Los Angeles as in Chicago, New York or Miami. This ensures voice privacy communications are available to individuals operating outside their home area during protracted surveillance or controlled deliveries.

The key definitions are as follows:

1. Key 1 will be "**BTS**" and will be installed in all ICE and CBP radios nationwide. *NOTE: This key replaces the old "CC" or Customs Common Key*
2. Key 2 will be defined as "**IOP**" (short for interoperability) and will be installed in all radios on the NLECC network. This key will primarily be utilized to communicate with non-DHS law enforcement agencies. *NOTE: This key is the same as the old INTEROP Key.*
3. Key 3 will be defined as "**INV TACT**" (for all ICE personnel) or "**OFO TACT**" (for all CBP personnel) and will be utilized to communicate with other officers within one's own organization. *NOTE: "INV TACT" replaces the old "OI TAC" and "OFO TACT" replaces the old "OFO TAC".*
4. Keys 4 – 8 are undefined and reserved for special operation.

National Key Standards – Non-DHS Users

Non-DHS Users on the NLECC network will utilize a standard series of voice privacy keys. The Key definitions are as follows:

1. Key 1 will be defined as the Agency Key, for installation in all radios nationwide for that agency. As an example, the USDA would have the "USDA" common key, while the FDA would have the "FDA" common key.
2. Key 2 will be defined as "**IOP**" and will be the interoperability key installed on all radios on the NLECC network. This key will primarily be utilized to communicate with DHS law enforcement agencies. ***NOTE: this is the Key to be utilized when calling Sector.***
3. Keys 4 – 8 are undefined and reserved for special operation

Key Management Considerations in Operational Planning

- Roaming from one KMC area to another. Since the majority of voice privacy keys in use by the NLECC are national in scope, the only time a unit should have to be roamed (transferred from one KMC to another) is when the user's radio loses encryption capability outside of its home KMC area. Appendix D shows the area of responsibilty of each KMC. Should roaming become necessary, simply advise Sector and ask to be roamed and re-keyed.

- Radios must be checked to ensure that the appropriate keys are loaded, and current prior to the commencement of the operation. It is strongly recommended that all radios to be used in an operation have a voice privacy radio check completed with Sector prior to commencing the operation.

- Limited Use Tactical Keys. Operation planners may decide the sensitivity of the operation dictates the use of a special or tactical voice privacy key for the duration of the operation. If a tactical voice privacy key is required, contact the Key Management Administrator at the NLECC to discuss limitations and implementation processes.

Lost or Stolen Radios

In addition to other prescribed procedures for reporting lost or stolen equipment, the loss of an OTAR capable radio should immediately be reported to the Key Management Administrator at the NLECC. There are two basic reasons for making this report. First, the Administrator may be able to turn off or "kill" the radio if it is turned on, and on a Net channel. This will prevent unauthorized personnel from intercepting sensitive communications. Second, if the radio is known to be in the hands of counter law enforcement personnel, the Administrator can implement an emergency key change, thus making the stolen radio useless in the interception of protected transmissions.

Changes in Radio Ownership

Changes in radio (or vehicle with radio installed) ownership should be reported to the Key Management Administrator at NLECC. This will permit updating of the KMC database with current information.

Radio Maintenance

If problems are encountered with your radio, or if the radio is inoperative, the equipment should be turned over to an authorized contractor for repair in accordance with the national maintenance contract.

Mobile Radios

Will be taken to an authorized Motorola Service Center in your area. All work performed upon the radio (except antennas) is normally covered under NLECC national maintenance contract, and therefore your office should not incur any fiscal responsibility for these repairs. Replacement antennas are generally available from the National Law Enforcement Communications Center High Tech Facility. This facility should be contacted at (407) 975-1100 for information on replacement antennas and installation procedures.

Portable Radios

All maintenance on portable radios is performed at the National Law Enforcement Communications Center High Tech Facility located in Orlando Florida. Defective or broken radios must be forwarded to this facility for repair. Radios will usually be repaired and returned to the forwarding office within five business days after receipt. When forwarding radios for repair, insure written information accompanies the radio defining the malfunction, user's name, address, and contact telephone number.

Preventative Maintenance & Inspection (PMI)

Each mobile and portable radio should receive a PMI annually. These inspections ensure radios continue to function in an optimum manner. In the event repairs or adjustments are necessary, they will be performed during these inspections. The authorized Motorola Service Center in your area will perform inspection of mobile radios. It is suggested the service center be contacted for an appointment to schedule this service. All PMI of portable radios is accomplished at the High Tech Facility in Orlando, Florida. It is recommended offices forward ten percent of their assigned portable radios each month for this inspection. Most PMIs are covered under the national maintenance contract; therefore offices will not incur any cost for these inspections. Questions regarding PMIs may be directed to the High Tech Facility or your Field Liaison Officer.

Appendix A - Law Enforcement Database Queries

TECS (Treasury Enforcement Communications System)

- Contains information on people, vehicles, vessels, aircraft, etc, specifically as it relates to Department of Treasury violations. Dissemination of this information is restricted.

NCIC (National Crime Information Center)

- Maintained by the FBI, this national system contains information on wanted/missing persons, criminal histories, stolen vehicles / vessels / guns, as well as many other items, too numerous to list.

NLETS (National Law Enforcement Telecommunications System)

- A national switching center, connecting NCIC with state and local law enforcement database systems.

CPIC (Canadian Police Information Center)

- Contains information on Canadian wanted persons, stolen property, etc.

INTERPOL (International Police)

- Contains information on international wanted persons, stolen property, etc.

NICB (National Insurance Crime Bureau)

- Contains information on automobile theft, insurance fraud, etc.

CLETS (California law Enforcement Telecommunications System)

- California state system that contains all state related information (vehicle/vessel registrations, driver's license info, state warrants, etc.)

FCIC (Florida Crime Information Center)

- Florida state system that contains all state related information (vehicle/vessel registrations, driver's license info, state warrants, etc.)

TLETS (Texas Law Enforcement Telecommunications System)

- Texas state system that contains all state related information (vehicle/vessel registrations, driver's license info, state warrants, etc.)

NYSPIN (New York State Police Information Network)

- New York state system that contains all state related information (vehicle/vessel registrations, driver's license info, state warrants, etc.)

MOTION (Metro Orleans Total Information Online Network)

- Louisiana state system that contains all state related information (vehicle/vessel registrations, driver's license info, state warrants, etc.)
-

LEAPS (Law Enforcement Agency Processing System)

- Massachusetts state system that contains all state related information (vehicle/vessel registrations, driver's license info, state warrants, etc.)

ATS/P (Automated Targeting System)

- Tracks the travel of international visitors, also contains violator and suspect records from U.S. and foreign sources.

Internet Queries

National Marine Fisheries

- www.st.nmfs.gov/st1/commerical access to vessel information through vessel name and U.S. Coast Guard documentation number.

Internet Fraud Complaint Center

- www.ifccfbi.gov IFCC provides statistical data on current fraud trends.

Canada 411

- www.canada411.sympatico.ca (Canadian PhoneDisk Directory)

Global Phone Directory

- www.globalyp.com/world.htm various state and local websites access to multiple law enforcement websites.

INS LESC

- (Investigative and Naturalization Service LE Support Center) INS database that provides U.S. status on foreign nationals.

NADDIS (Narcotics and Dangerous Drugs Information System)

- Obtained through EPIC (El Paso Intelligence Center) contains historical and current data on DEA cases and those of other Federal Law Enforcement Agencies.

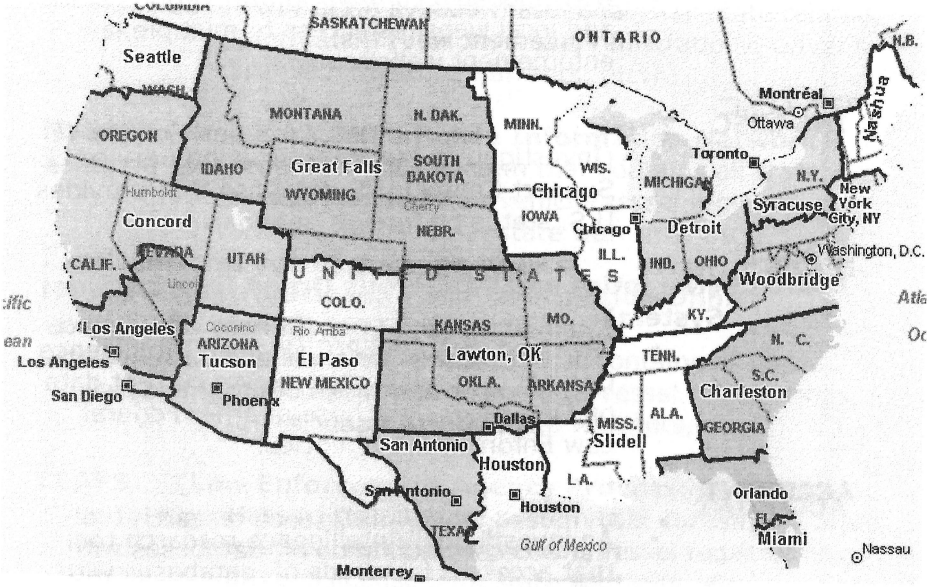
ACCURINT

- An investigative/intelligence research tool that accesses hundreds of databases with billions of records in order to locate people, businesses and their assets. Find deep background and historical information, associates and relatives.

BLIS (Blue Lightning Information System)

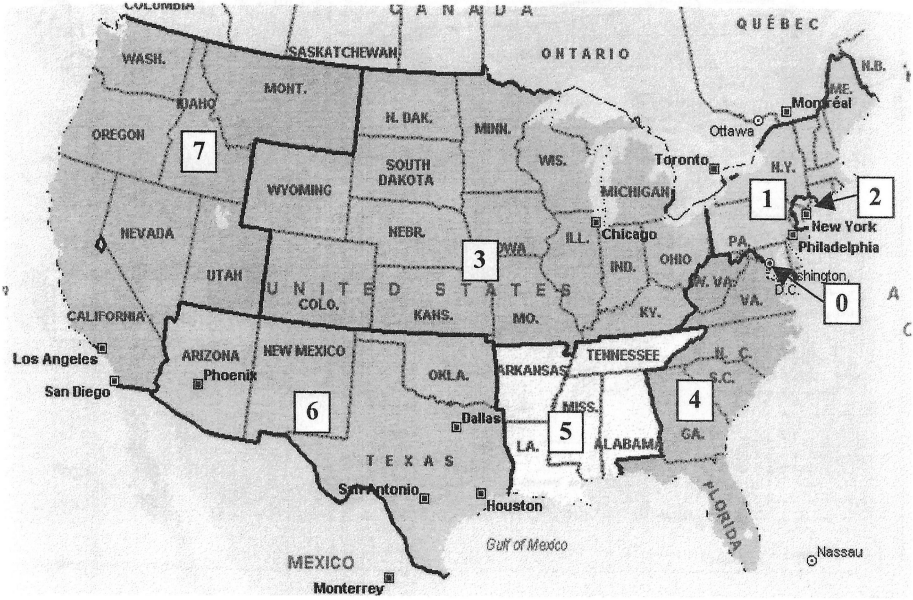
- Maintained by the South Florida Investigative Support Center. A Marine database containing records on vessel boarding, sightings and private vessel reports in the South Florida area.

Appendix B – NLECC Radio Shops



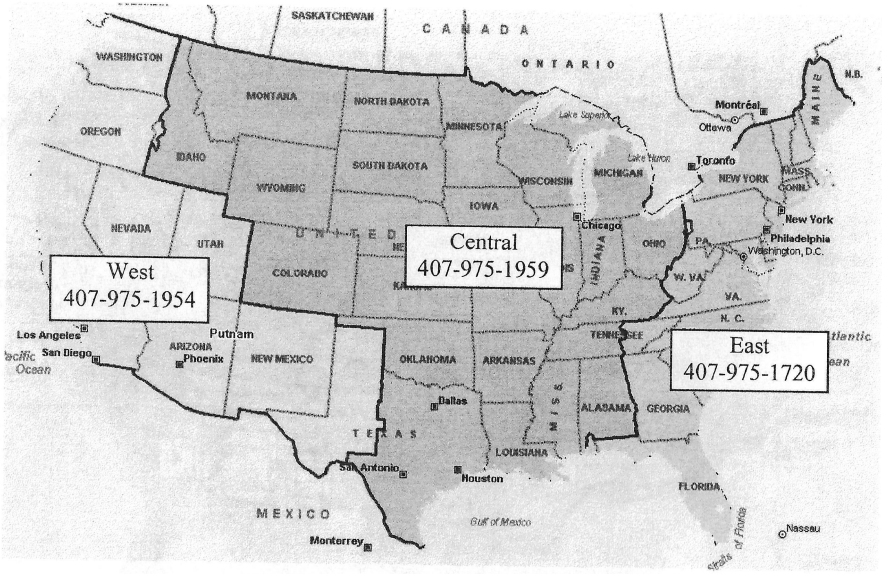
Charleston	Chicago	Concord	Detroit
(843) 760-9525	(630) 628-0428	(925) 798-4693	(248) 669-1099
EL Paso	*Everett*	*Great Falls*	*Honolulu*
(915) 633-7340	(360) 647-0119	(406) 452-8028	(808) 861-4200
Houston	*Lawton*	*Long Beach*	*Miami*
(713) 718-3130	(580) 353-5064	(909) 305-1657	(305) 597-4680
Nashua	*New York*	*Orlando (NLECC)*	*San Antonio*
(603) 886-1593	(718) 539-4370	(407) 975-2000	(210) 295-9577
San Diego	*Slidell*	*Syracuse*	*Tucson*
(619) 671-4500	(504) 733-0823	(315) 463-9855	(520) 670-6720
Woodbridge			
(703) 495-6019			

Appendix C – Sector Radio Callsign prefixes



NLECC Network Callsign Agency Identifiers			
DHS Users		Other Agency Users	
A	Investigations	ATF	Alcohol Tobacco and Firearms
B	Headquarters	BIA	Bureau of Indian Affairs
C	Communications	BP	U.S. Border Patrol
D	Port Headquarters	CG	U.S. Coast Guard
E	Applied Technology	CIA	Central Intelligence Agency
I	Field Operations	DEA	Drug Enforcement Administration
K	Canine Enforcement	DOD	Department of Defense DCIS
L	Aviation Personnel	F	Health and Human Services
M	Marine Operations	FEMA	Federal Emergency Manage Agency
O	Aircraft	INS	Immigration and Naturalization Service
R	CMC	NPS	National Park Service
S	Internal Affairs	P	IRS – Inspector General
T	Task Force	V	Housing and Urban Development
X	Reserved (Temp Callsign)	Y	Treasury – Office of the I.G.

Appendix D –OTAR Area of Responsibility

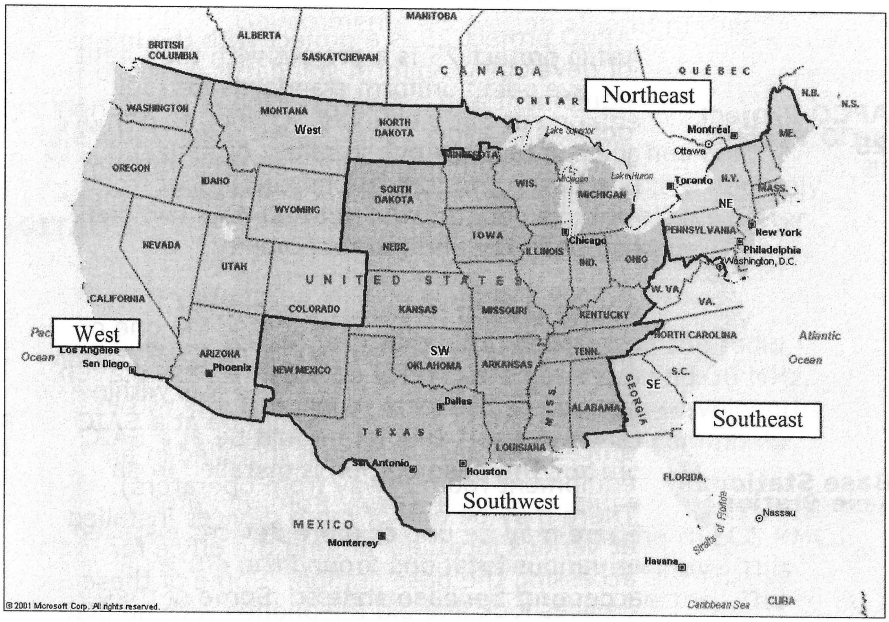


OTAR Area of Responsibilities		
West	**Central**	**East**
(407) 975-1954	(407) 975-1959	(407) 975-1720
National Toll- Free Hotline	**800-326-5322**	

Three KMC (Key Management Controller) Specialists are responsible for all aspects of the national Over-The-Air-Rekey program. Their primary functions include:

- Coordinating all aspects of key management and voice privacy communications within a particular area of responsibility.
- Developing key management plans, policies and agreements for supporting authorized users.
- Acting as the technical experts in all OTAR related matters.
- Introducing, implementing and maintaining nationwide voice-privacy keys, and ensuring compliance with national standards.

Appendix E –FLO Area of Responsibility



Field Liaison Office Locations			
Northeast	**Southeast**	**Southwest**	**West**
New York	*Orlando*	*Houston*	*Spokane*
(843) 760-9525	**(630) 628-0428**	**(925) 798-4693**	**(248) 669-1099**

The four Field Liaison Officers work under the direction of the Tactical Communications Group Supervisors. They are primarily responsible for:

- Meeting with Field managers to assist with planning tactical communications aspects of enforcement operations.
- Managing and providing user training under the Tactical Communications Field Refresher Training Program within their area of responsibility.
- Assisting the Tactical Communications Group Supervisors with Liaison visits at user offices.

APCO Project 25	APCO project 25 is a project with the intent of developing uniform standards for radio equipment and networks. One of its primary goals is to allow public safety organizations to purchase communications equipment from multiple vendors and yet maintain complete compatibility and interoperability.
Base Station	A base station is usually a remotely controlled radio that is accessed via one or more remote control devices. A base station can access the local repeater if it is within range. A good example would be at a SAIC office. The base station is installed in an equipment room (away from operators). There may be one or more devices installed at various locations around the office for accessing the base station. Some of these devices look like old telephones with no dial pads.
Coded	Also known as 10-10, encrypted, secure, cypher or green. This means you are transmitting using a digital signal to secure the information passed.
Consolette	A desktop radio incorporating a transmitter, receiver and control panel all in one package. This setup requires an outside mounted antenna.
COTHEN	Customs Over the Horizon Enforcement Network. Customs High Frequency (HF) radio network, used primarily by U.S. Customs Air and Marine Programs. The COTHEN program is located at the NLECC.
CSK	Common Shadow Key. Common shadow keys are used to encrypt the rekey message sent to a group of radios.

DES	Data Encryption Standard – The U. S. Governments encryption algorithm that allows secured voice and data communications.
DIGITAC	A repeater system that usually has one transmitter, but two or more active remotely located receivers. This system allows better radio coverage in some of the large metropolitan areas.
HF	High Frequency. That portion of the radio frequency spectrum between 3 and 30 MHz. This frequency characterized by wavelengths between 10 and 100 meters, is commonly called the Short Wave Band.
Inhibit / Enable	When a radio is lost or stolen the NLECC KMC team should be notified immediately. This can be accomplished through Sector. The radio in question can be set to inhibit, which will effectively turn the radio off at its next encounter with the KMC. However, this means that the radio must be on the USCS network channel to communicate with the KMC. Conversely when a radio is recovered it can be enabled from the KMC.
KLK	Key Loss Key – The method, through OTAR or wireline, that a current key is restored to a DES/OTAR equipped radio that already contains or contained that key.
KMC	Key Management Controller – The computer system that manages the U.S. Customs Service's use of DES keys. This system permits the transfer, loading and replacement of voice privacy keys in large groups of radios.

KVL	Key Variable Loader. Hand held device used to physically transfer encryption keys to radios.
MDCID	Motorola Data Control ID. The MDCID is the hexadecimal electronic ID transmitted by each radio and is used by the KMC to determine whether any key management messages are pending. Also see UID.
NCIC	National Crime Information Center. A nationwide, computerized information system established as a service to all criminal justice agencies; local, state and federal. The NCIC System serves criminal justice agencies in the 50 states, the District of Columbia, U.S. Territories and Canada. The FBI is the manager of the NCIC System.
NET	Preprogrammed repeater channels that facilitate radio operation on the NLECC VHF repeater NETwork.
NLECC	National Law Enforcement Communications Center. Commonly called "Sector", the NLECC is actually composed of several tactical communications entities and programs.
OTAR	Over The Air Rekeying – The ability to securely transmit DES (or other) keys over the air for updates or in the event of lost codes (dead batteries).
PCA	Pre-Clearance Alert. The Pre-Clearance Alert System provides inspectors at pre-clearance sites the ability to send advance NCIC wanted fugitive warning to specific destination airports in the U.S. and Sector Communications.

PROM	Programmable Read Only Memory – Also known as EPROM or EEPROM. This is the method whereby Tactical Communications Officers can program what channels and functions are available on any given radio.
PTT	Push To Talk – The function of placing a radio in the "transmit" mode by pushing a button. PTT sends the radio's UID to SECTOR for ID and OTAR purposes.
Query Notify 2	Notification to the TECS record owner and to a 24-hour backup (Sector Communications).
ReKey	The method, through OTAR or Wireline, that a new version of a key is downloaded into a DES/OTAR equipped radio.
Repeater	A radio (usually fixed site, sometimes movable) that simultaneously rebroadcasts the signal (singular) it receives. All user radios that are on the repeater channel (NET) and are within range will hear the repeated signal, thus improving the operating range in most situations.
Request Rekey	A radio user may request a re-key either via voice request to Sector or manually from the key pad or from the ASN box. Rekeys can also be initiated by the KMC.
Roaming	The electronic transfer of a user radio from one KMC region to another. This permits KMC ID and other OTAR actions to be performed while out of the home user area.
Sector	Located at the NLECC. Sector is CBP's primary national radio network and tactical communications center.

Signal	Located at the NLECC. Customs Message Center. Handles the transmitting and receiving of Classified and Unclassified message traffic.
Simplex	Communications conducted directly from one unit to one or more other units without the use of a repeater. When the other desired users are within range, this mode of communications is less likely to interfere with other users. A channel or frequency known as "car to car" is a good example of Simplex. Only one unit at a time may transmit. These Frequencies are referred to within U.S. Customs Service as "TAC" frequencies, and may vary from location to location.
TAC	Preprogrammed TACtical channels that allow simplex operation on the U.S. Customs Service VHF radio system
UID	Unit IDentification – A unique electronic ID number assigned during the programming of each radio. See also MDCID
USK	Unique Shadow Key. A Unique Shadow Key is an encryption key used to encrypt the transmission of traffic keys from the KMC to an individual radio. This prohibits the unauthorized reception of the traffic keys being distributed by the KMC.
VHF	Very High Frequency. That portion of the radio frequency spectrum from 30 to 300 MHz. Customs Repeaters utilize the VHF Spectrum.

INDEX

NLECC Network 10-Codes and Phonetic

10-1	Poor Radio Copy
10-2	Good Radio Copy
10-3	Stop Transmitting
10-4	Acknowledgement....
10-5	Relay To.....
10-6	Busy (Subject To Call)
10-7	Out Of Service
10-8	In Service
10-9	Repeat....
10-10	In The Coded Mode (D.E.S.)
10-12	Stand By
10-19	Return To....
10-20	Location....
10-21	Call....By Telephone
10-22	Disregard
10-27	Drivers License Information
10-28	Vehicle Reg. Information
10-29	Check For Wanted/Stolen
10-30	Unnecessary Use Of Radio
10-38	Vehicle Stop
10-39	Urgent - Use Light & Siren
10-40	Silent Run - No Light Or Siren
10-42	Residence
10-43	Information
10-59	Convoy, Escort, Surv.
10-61	Visiting Personnel
10-76	Enroute To....
10-84	Meet Me At.....
10-95	Prisoner/Subject Escort

A	Alpha
B	Bravo
C	Charlie
D	Delta
E	Echo
F	Foxtrot
G	Golf
H	Hotel
I	India
J	Juliett
K	Kilo
L	Lima
M	Mike
N	November
O	Oscar
P	Papa
Q	Quebec
R	Romeo
S	Sierra
T	Tango
U	Uniform
V	Victor
W	Whiskey
X	X-ray
Y	Yankee
Z	Zulu

This document was produced and distributed by the Training Unit of the National Law Enforcement Communication Center in Orlando, FL. To obtain additional copies, or to obtain other training related materials, contact:

NLECC Training Unit
1900 Lakemont Ave
Orlando, FL 32803
407-975-1010